AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/23/2024

Sign up

# Wireshark training

3 days (21 hours)

## Presentation

Our Wireshark training course will immerse you in the exciting world of network analysis, equipping you with the knowledge and skills you need to master this cutting-edge technology.

This training program covers a wide range of topics, from an introduction to Wireshark to advanced aspects such as packet analysis, network anomaly detection and performance troubleshooting.

You'll be introduced to the fundamental concepts of network analysis, and explore the different applications in various industrial sectors, from cybersecurity to enterprise network management.

With our training course, you'll learn how to use Wireshark's advanced features to efficiently capture, filter and analyze network traffic.

You'll also discover how to interpret captured data to identify performance problems, security flaws and suspicious behavior on the network.

As usual, we'll be using the latest stable version and resources of Wireshark.

## Objectives

- Understanding the role of network forensics and its applications
- Master the use of custom capture and display filters
- Detect and analyze unencrypted traffic to identify vulnerabilities
- Perform email forensics with Wireshark
- Configure Wireshark for troubleshooting and network performance analysis

## Target audience

- Network administrators
- IT security engineers
- Network Performance Analysts

## Prerequisites

- Basic knowledge of networks and TCP/IP protocols is recommended
- Prior knowledge of network analysis tools would also be beneficial.

## OUR WIRESHARK TRAINING PROGRAM

### INTRODUCTION TO FORENSIC NETWORKING

- Understanding the role of network forensics and its applications
- Discover the basic principles and functions of Wireshark
- Install Wireshark and familiarize yourself with the user interface
- Configure basic options for packet capture
- Learn how to navigate the different Wireshark windows

### ADVANCED WIRESHARK SETTINGS

- Create and use custom capture and display filters
- Manage and configure analysis profiles for different use cases
- Mastering command-line network capture commands with Tshark
- Understanding the importance of color in package analysis
- Save and share configurations for collaborative use

### ANALYSIS OF LAN SECURITY THREATS

- Detect and analyze unencrypted traffic to identify vulnerabilities
- Recognize sniffing attacks and network reconnaissance techniques
- Identify password-cracking attempts and other types of attack
- Use Wireshark's complementary tools for more in-depth analysis
- Design display filters to isolate and examine specific threats

### ANALYSIS OF EMAIL COMMUNICATIONS

- Perform email forensics with Wireshark
- Analyze attacks targeting email communications
- Understanding SMTP and other email protocols
- Use filters to isolate email traffic

- Study examples of phishing and spam

## MALWARE TRAFFIC INSPECTION

- Preparing the Wireshark environment for malicious traffic inspection
- Identifying the characteristics of IRC botnet traffic
- Use advanced filters to detect communication with command and control servers
- Reassembling data streams to extract malware
- Analyze packets for anomalies and signals of malicious activity

## NETWORK PERFORMANCE ANALYSIS

- Configure Wireshark for troubleshooting and network performance analysis
- Understand and analyze TCP/IP connection problems
- Use statistics and graphics to identify bottlenecks
- Run diagnostics on network application performance
- Optimize the network by identifying lost packets, retransmissions and latencies

## NETWORK FUNDAMENTALS

- Review the key concepts of network communications, topologies and the OSI model
- Examine Ethernet frame format and the ARP protocol
- Understanding the different layers of the OSI model and how they interact
- Learn to interpret Layer 2 and Layer 3 protocol information
- Routing and flow control protocols

## USING THE WIRESHARK INTERFACE

- Explore toolbar and status bar functions in detail
- Apply and customize filters to improve packet analysis
- Examine package contents in detail
- Use flow tracking functions to analyze specific conversations
- Manage annotations and markers to facilitate subsequent analysis

## ANALYSIS AND TROUBLESHOOTING TASKS WITH WIRESHARK

- Capture and analyze network traffic to identify security and performance problems
- Reassemble files and listen to VoIP communications
- Identify and solve TCP latency and performance problems
- Detect application errors and congestion problems
- Use advanced techniques for security analysis, including suspicious traffic identification and network reconnaissance

# Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.